

Claims

- 1 1. A process for configuring, across the Internet, a digital certificate
- 2 for a network device, the process comprising:
 - 3 building a secret data encryption key into a network device when the
 - 4 network device is manufactured;
 - 5 maintaining the secret key and a corresponding unique identifier of the
 - 6 network device in a database server accessible over the Internet;
 - 7 sending, across the Internet from the network device to the database
 - 8 server, a two-part message wherein the first part contains the unique identifier,
 - 9 the IP address of the network device and a request for a digital certificate, and
 - 10 wherein the first part is encrypted using the built-in secret key, and wherein
 - 11 the second part of the message has at least some of the same information as the
 - 12 first part of the message, including the unique identifier, but is not encrypted;
 - 13 determining, by the database server, the secret key from the database
 - 14 using the unique identifier received in the second part of the message;
 - 15 decrypting, using the secret key from the database, the first part of the
 - 16 message;
 - 17 comparing the information in the decrypted first part of the message with
 - 18 the information in the second part of the message;

19 comparing the IP address from which the message was received and the
20 IP address specified in the message; and
21 sending a digital certificate to the network device if the information
22 matches and the IP addresses match.

10004516-116201

23 2. A process for configuring a digital certificate for a network device
24 in a network environment, the process comprising:
25 embodying a secret key into the device;
26 storing, by an entity responsible for embodying the secret key, the secret
27 key and a unique identification number of the device in a secure database
28 accessible by the entity and a certificate authority;
29 receiving, by a certificate authority, a two-part message from the network
30 device requesting a digital certificate wherein the first part of the message
31 includes the unique identification number and the second part of the message is
32 an encryption of the first part of the message encrypted with the secret key;
33 determining, by the certificate authority, the secret key from the
34 database using the unique identification number;
35 decrypting, using the secret key from the database, the second part of the
36 message;
37 comparing the decrypted message with the first part of the message; and
38 sending a digital certificate to the network device if the two parts match.

1 3. The process of claim 2 wherein the network device is a fax
2 machine.

1 4. The process of claim 2 wherein the network device is a printer.

1 5. The process of claim 2 wherein the network device is a modem.

1 6. The process of claim 2 wherein the entity embodying the secret key
2 and the certificate authority are a same entity.

1 7. The process of claim 2 wherein the entity embodying the secret key
2 is a manufacturer of the network device, and wherein the secret key is
3 embodied in the device when the device is manufactured.

2 8. A network device having a unique identification number, the
3 network device comprising:
4 a secret key embodied in said network device when the network device is
5 manufactured;
6 means for generating a two-part message requesting, from a digital
7 authority, a digital certificate wherein the first part of the message includes the
8 unique identification number and the second part of the message is an
9 encryption of the first part of the message using the secret key; and
 means for receiving a digital certificate.

1 9. The network device of claim 8 wherein the network device is a
2 printer.

1 10. The network device of claim 8 wherein the network device is a fax
2 machine.

1 11. The network device of claim 8 wherein the network device is a
2 modem.

10004516-310204

1 12. A computer system having a database, the computer system
2 comprising:
3 means for receiving a secret key and a corresponding unique
4 identification number of a network device from an entity responsible for
5 embodying the secret key into the network device;
6 means for storing the secret key and the corresponding unique
7 identification number in the database;
8 means for receiving a two-part message from the network device
9 requesting a digital certificate wherein a first part of the message includes the
10 unique identification number and the second part of the message is an
11 encryption of the first part of the message encrypted by the network device
12 using the embodied secret key;
13 means for accessing the database to find the secret key associated with
14 the unique identification number from the first part of the message;
15 means for decrypting the second part of the message using the secret key
16 from the database;
17 means for comparing the decrypted second part of the message with the
18 first part of the message; and
19 means for sending to the network device a digital certificate if the
20 decrypted part of the message matches the first part of the message.

1 13. A computer program, on a computer-usable medium, comprising:
2 means for enabling receipt of a secret key and a corresponding unique
3 identification number of a network device from an entity responsible for
4 embodiment of the secret key into the network device;
5 means for causing the secret key and the corresponding unique
6 identification number to be stored in a database;
7 means for enabling receipt of a two-part message from the network device
8 requesting a digital certificate wherein a first part of the message includes the
9 unique identification number and the second part of the message is an
10 encryption of the first part of the message encrypted by the network device
11 using the embodied secret key;
12 means for causing an access to the database to find the secret key
13 associated with the unique identification number from the first part of the
14 message;
15 means for causing a decryption of the second part of the message using
16 the secret key from the database;
17 means for comparing the decrypted second part of the message with the
18 first part of the message; and
19 means for causing a digital certificate to be sent to the network device if
20 the decrypted part of the message matches the first part of the message.

1 14. A method executed in a computer system having a database, the
2 method comprising:
3 receiving a secret key and a corresponding unique identification number
4 of a network device from an entity responsible for embodying the secret key into
5 the network device;
6 storing the secret key and the corresponding unique identification
7 number in the database;
8 receiving a two-part message from the network device requesting a
9 digital certificate wherein a first part of the message includes the unique
10 identification number and the second part of the message is an encryption of
11 the first part of the message encrypted by the network device using the
12 embodied secret key;
13 accessing the database to find the secret key associated with the unique
14 identification number from the first part of the message;
15 decrypting the second part of the message using the secret key from the
16 database;
17 comparing the decrypted second part of the message with the first part of
18 the message; and
19 sending to the network device a digital certificate if the decrypted part of
20 the message matches the first part of the message.